REMARKS

Claims 1-2, 5-8, 10-28, 31-34, and 36-41 have been cancelled. Claims 3, 9, 29, and 35 have been amended to clarify the subject matter regarded as the invention. Claims 3, 4, 9, 29, 30, and 35 are pending.

The Examiner has rejected claims 3, 4, 9, 29, 30, and 35 under 35 USC 112, second paragraph. Independent claims 3, 9, 29, and 35 have been amended to delete the term "possible", which amendment is believed to overcome the rejections under 35 USC 112.

The Examiner has rejected claims 3, 4, 9, 29, 30, and 35 under 35 USC 102(e) as anticipated by Crosbie.

The rejection is respectfully traversed. With respect to claim 3, Crosbie teaches search for attack patterns to detect exploits. However, Crosbie does not describe using a regular expression to detect an sgid exploit by "searching for [log] entries showing that a process has been started by a sgid process with effective group ID equal to zero and group ID (gid) not equal to zero," as recited in claim 3. See, e.g., Crosbie at 50-54 (not listing sgid exploit among "Events Supported in Shipped Version"). Support for the amendment to claim 3 may be found, without limitation, in the Application at page 60, lines 4-19 and Figure 26. As such, claim 3 is believed to be allowable.

Claim 4 depends from claim 3 and is believed to be allowable for the same reasons described above.

Similarly to claim 3, claim 9 recites "searching for entries showing that the shell has started a process... wherein the shell comprises a sgid process with effective group ID equal to zero and group ID (gid) not equal to zero." As such, claim 9 is believed to be allowable for the same reasons described above.

Similarly to claim 3, claim 29 recites a processor "configured to search for entries showing that a process has been started by a sgid process with effective group ID equal to zero

and group ID (gid) not equal to zero." As such, claim 29 is believed to be allowable for the same reasons described above.

Claim 30 depends from claim 29 and is believed to be allowable for the same reasons described above.

Like claim 3, claim 35 recites "searching for [log] entries showing that a process has been started by a sgid process with effective group ID equal to zero and group ID (gid) not equal to zero." As such, claim 35 is believed to be allowable for the same reasons described above.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: 10/13/04

William J. James
Registration No. 40,661
V 408-973-2592
F 408-973-2595

VAN PELT AND YI, LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014

2136

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Sorkin	Examiner:	Ronald Baum
Application No.:	09/841,689	Art Unit:	2136
Filed:	April 23, 2001	Docket No.:	RECOP008
Title:	SYSTEM AND METHOD FOR ANALYZING LOGFILES		

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in a prepaid envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

October 13, 2004.

Vicki Lorist

TRANSMITTAL FOR AMENDMENT B

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Sir:

Transmitted herewith is an amendment in the above-identified application.

The fee has been calculated as shown below.

	Claims remaining after Amendment		Highest previously paid for	Present Extra		Small Entity			Large Entity	
						Rate	Additional Fee		Rate	Additional Fee
Total Claims	6	Less	41			x $9 = $		OR	x $18 = $	
Indep Claims	4	Less	13			x $43 = $		OR	x $86 = $	
[ ]Multiple Dependent claim Present & Fee Not previously paid						x $145 = $		OR	x $290 = $	
						TOTAL ADD'L FEE $			TOTAL ADD'L FEE $	

☒ Applicant(s) hereby petition for a **TWO** month(s) extension of time to respond to the outstanding Office Action.

☒ Applicant(s) believe that no (additional) Extension of Time is required; however, if it is determined that such an extension is required, Applicant(s) hereby petition that such an extension be granted and authorize the Commissioner to charge the required fees for an Extension of Time under 37 CFR 1.136 to Deposit Account No. 50-0685. ( ).

☒ Enclosed is our Check No. 1445 in the amount of $430 to cover the additional claim fee and/or extension of time fees.

☐ Enclosed is Applicant Initiated Interview Request Form, PTOL-413A.

☐ Enclosed are _____sheets formal drawings.

☐ Please charge Deposit Account No. 50-0685 ( ) in the amount of $_____to cover the additional claim fee and/or extension of time fees.

☒ If the required fees are missing or any additional fees are required during the pendency of the subject application, please charge such fees or credit any overpayment to Deposit Account No. 50-0685 (RECOP008).

Respectfully submitted,

Dated: 10/13/04

William J. James
Registration No. 40,661
V 408-973-2592
F 408-973-2595

VAN PELT AND YI, LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014